RSAC 2025 Conference

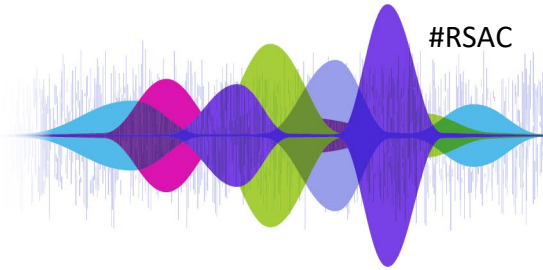
Many Voices.
One Community.

SESSION ID: DSA-M01

A Stuxnet Moment for Supply Chain Security?

Andrea Little Limbago, PhD

SVP, Applied AI
interos.ai
https://www.linkedin.com/in/andrea-little-limbago/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The Pager Attacks: A Brief Overview

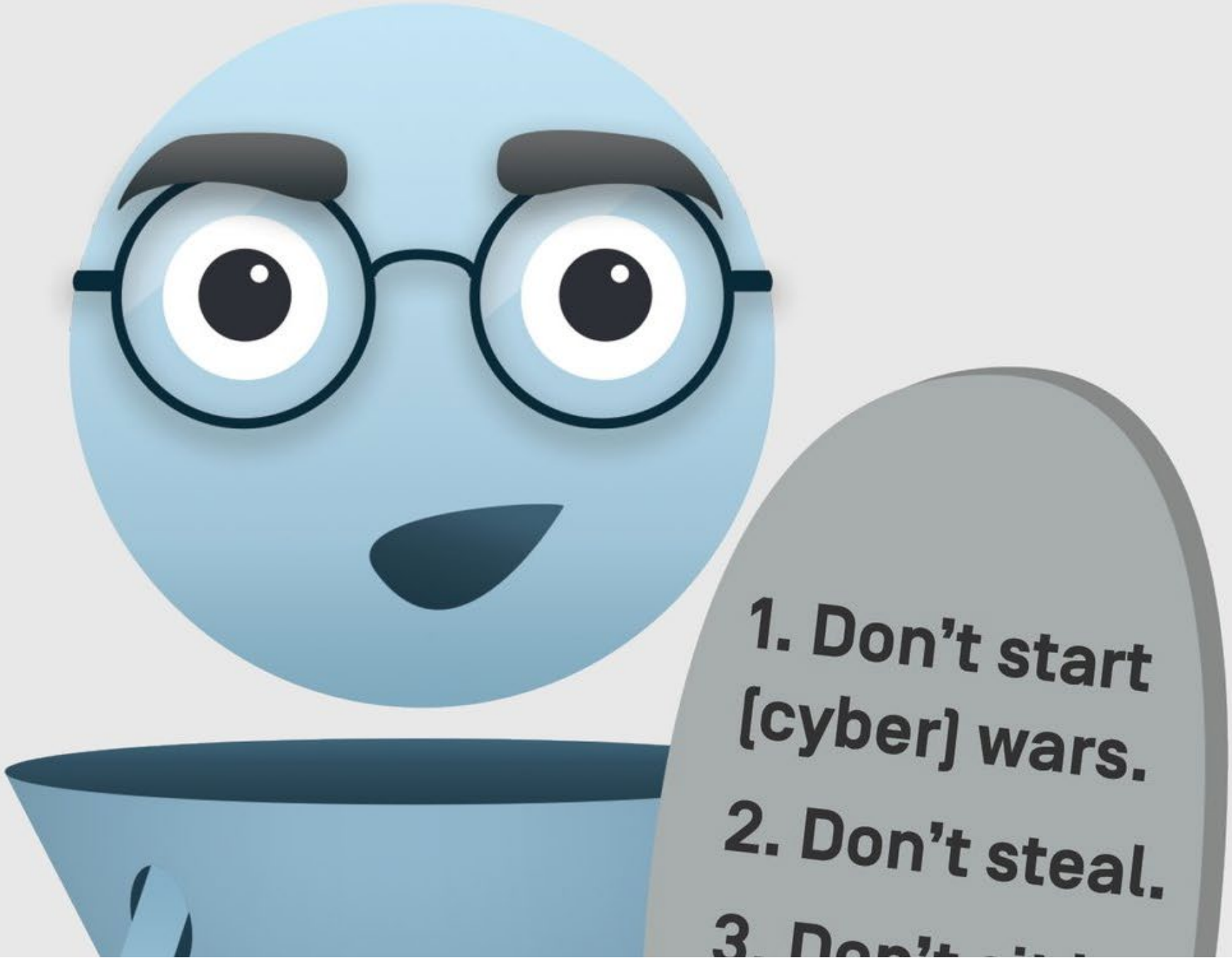
- **September 2024**: Explosives planted in Hezbollah pagers and walkie talkies, killing dozens and injuring thousands
- Global supply chains infiltration is not new:
  - Plastic explosives
  - Cellphones booby trapped
  - Tech backdoors
  - Front companies
- Lethality of the attack within hyperspecialized and complex supply chains….is new

“One of the most unprecedented cyber-attacks seen in warfare?” An inflection point in supply chain infiltration?

https://www.consultancy.eu/news/10680/the-murky-trail-of-hezbollahs-exploding-pagers-to-a-hungarian-consulting-firm

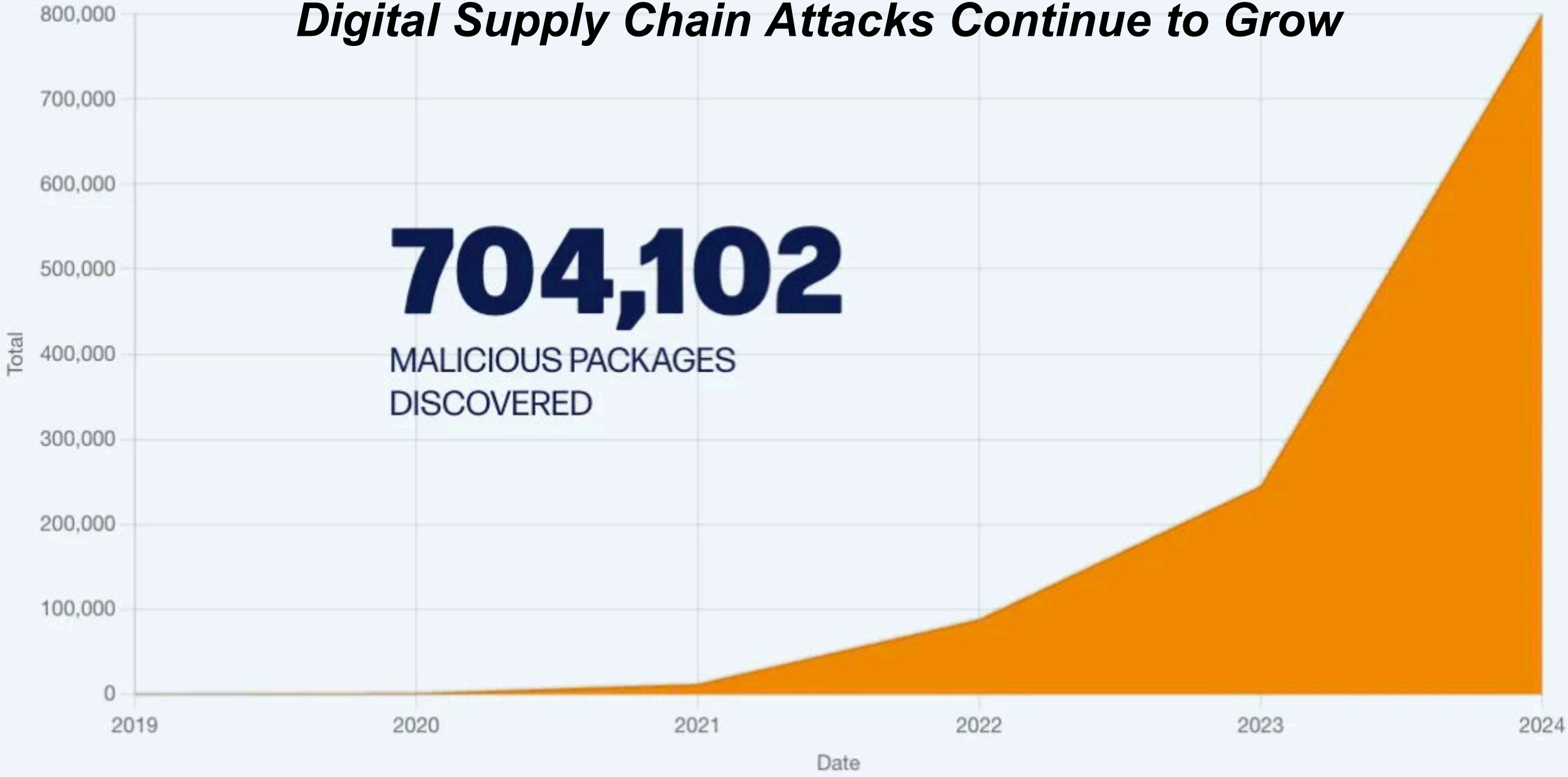
What are norms?

Cyber norms: voluntary guidelines that outline how states should behave in cyberspace.



https://www.newamerica.org/cybersecurity-initiative/policy-papers/professor-cy-burrs-graphic-guide-international-cyber-norms/

Digital Supply Chain Attacks Continue to Grow



Source: Sonatype
https://www.resilientcyber.io/p/2024-state-of-the-software-supply

“But now that the line has been crossed, other countries will almost certainly start to consider this sort of tactic as within bounds.”

Bruce Schneier, NYTimes

https://www.nytimes.com/2024/09/22/opinion/israel-pager-attacks-supply-chain.html

RSAC 2025 Conference

Pager Attacks: Brief Overview

First Stop: Taiwan

'This is very embarrassing': Middle East crisis takes a detour to an office park in Taiwan

- Pager Model numbers AR924 linked to Taiwanese tech company, Gold Apollo
  - Gold Apollo authorizes companies to use their trademark in certain regions
  - Taiwan's Economic Affairs Ministry said Wednesday that Gold Apollo had exported 260,000 pagers from 2022 to August 2024
- "The design and manufacturing of the products are solely the responsibility of BAC," a Gold Apollo statement
  - Taiwan heavily regulates the shipments of pagers, and the Ministry of Affairs has no record of Gold Apollo pagers being shipped to Lebanon
- Pointed to BAC Consulting in Hungary
  - Claims they wanted to make their own pagers and use the logo

Next Stop: A Shell Company in Hungary?

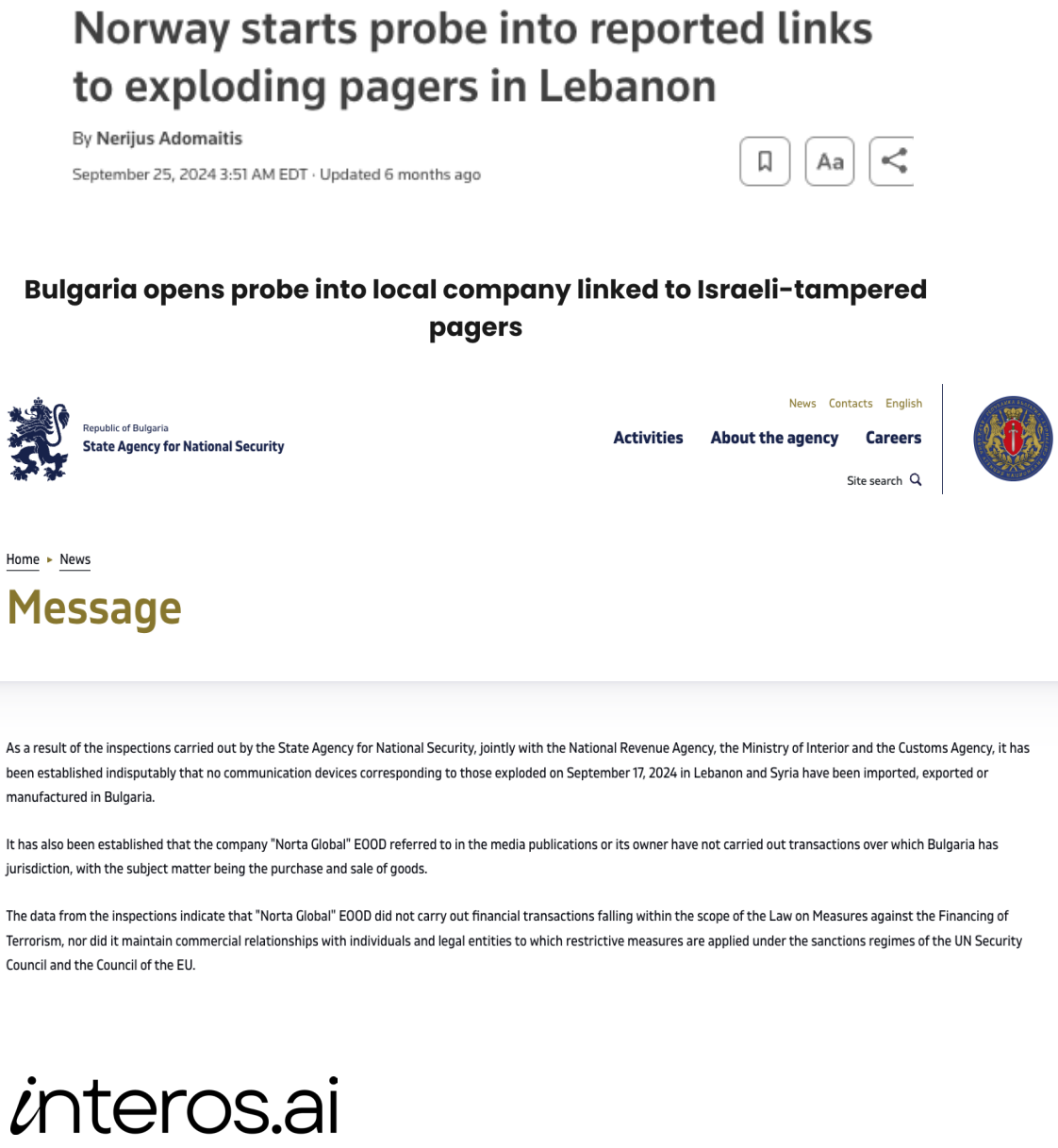
"The referenced devices have never been in Hungary," Hungary's State Secretary for International Communication Zoltan Kovacs said.

https://www.dw.com/en/two-european-firms-in-focus-of-hezbollah-pager-explosions/a-70248830

- BAC Consulting contracted with Gold Apollo ~2021-22
  - Conducted genuine sales during this time
  - In corporate registry, listed 118 functions from sugar and oil production to natural gas
  - No manufacturing or operational site in Hungary
- Reporters found no evidence of a company, but rather a piece of paper
- Website deleted September 18

Reached by phone Wednesday, BAC Consulting Chief Executive Cristiana Bársony-Arcidiacono confirmed that her company worked with Gold Apollo. But when asked about the pagers and the explosions, she said, "I don't make the pagers. I am just the intermediate. I think you got it wrong."

Or was it a Bulgarian tech firm with a Norwegian founder?



Norway starts probe into reported links to exploding pagers in Lebanon

By Nerijus Adomaitis

September 25, 2024 3:51 AM EDT · Updated 6 months ago

Bulgaria opens probe into local company linked to Israeli-tampered pagers

Republic of Bulgaria
State Agency for National Security

News Contacts English

Activities About the agency Careers

Site search

Home ▸ News

Message

As a result of the inspections carried out by the State Agency for National Security, jointly with the National Revenue Agency, the Ministry of Interior and the Customs Agency, it has been established indisputably that no communication devices corresponding to those exploded on September 17, 2024 in Lebanon and Syria have been imported, exported or manufactured in Bulgaria.

It has also been established that the company "Norta Global" EOOD referred to in the media publications or its owner have not carried out transactions over which Bulgaria has jurisdiction, with the subject matter being the purchase and sale of goods.

The data from the inspections indicate that "Norta Global" EOOD did not carry out financial transactions falling within the scope of the Law on Measures against the Financing of Terrorism, nor did it maintain commercial relationships with individuals and legal entities to which restrictive measures are applied under the sanctions regimes of the UN Security Council and the Council of the EU.

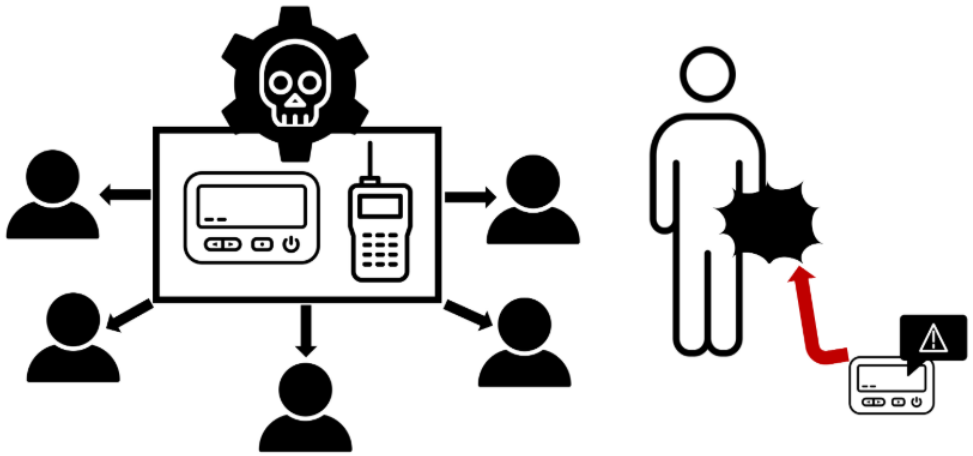
- Hungarian news reported that BAC Consulting was an intermediary and pointed to Bulgarian company Norta Global as the manufacturer
- Sofia-based Norta Global Ltd was investigated for selling the pagers to Hezbollah
  - BAC Consulting self-described as the ‘intermediary’, only manufactured on paper, but logistics handled by Norta Global?
- Bulgarian state security agency did not detect any shipments of pagers
- Norta Global – founded in 2022 – by a Norwegian citizen
  - His LinkedIn profile showed employment at DN Media Group since 2020, then disappeared following the attacks
  - Bulgarian records showed the company had no employees, and is operating from an address linked to Agentsya Za Novy Firmy (another shell company?)

interos.ai

RSAC 2025 Conference

Supply Chain Distribution

I-B *The Pager and Walkie-Talkie Attacks*



(a) Distribution of Malicious Pagers & Walkie-talkies (b) The explosion

Figure 1: A brief overview of the pager and walkie-talkie attacks

https://arxiv.org/html/2501.17405v1

- Hezbollah reportedly thought they were buying pagers from Gold Apollo
- Thousands of pagers purchased from Europe, under Gold Apollo license
  - Numbers range from 5000-16000
  - Booby-trapped pagers had 3 grams of explosives
  - Error message sent to pagers caused a vibration and exploded when users tried to silence them
- Former Hezbollah leader, Hassan Nasrallah, urged members to use pagers instead of mobile phones to prevent tracking and monitoring
  - Killed in an airstrike shortly after the pager attacks
- Still unclear whether pagers were tampered with or infiltrated from the beginning
- FEB 25: According to Mossad Director, David Barnea, first pagers and walkie-talkies arrived in Lebanon in September 2023

“These attacks represent a new development in warfare, where communication tools become weapons, simultaneously exploding across marketplaces, on street corners, and in homes as daily life unfolds,” UN human rights chief Volker Türk told the Security Council.

https://www.cnn.com/2024/09/27/middleeast/israel-pager-attack-hezbollah-lebanon-invs-intl/index.html

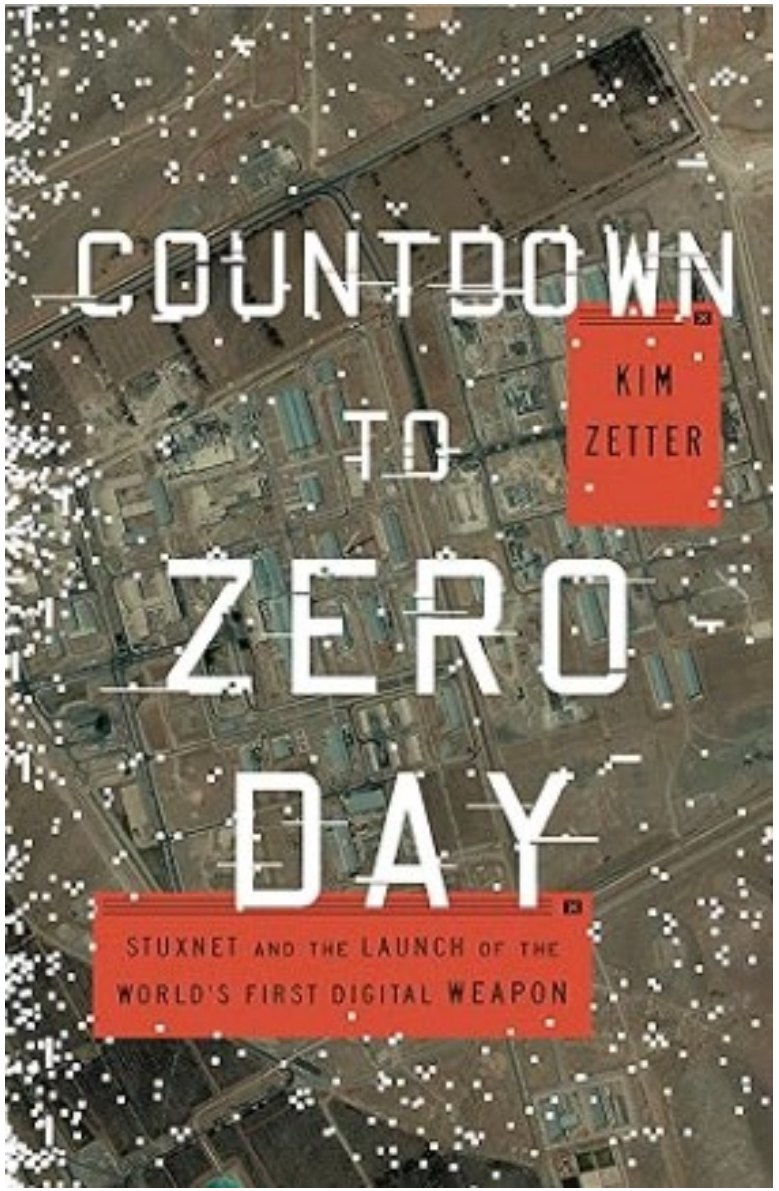
RSAC 2025 Conference

Is this a New Era of ‘Supply Chain Warfare’?

And is this a new Stuxnet Moment?

Many Voices.
One Community.

Stuxnet inflection point & cyber norms



- Stuxnet is often described as the first use of cyber as a weapon for physical destruction and geopolitical motivations
- 15 years later, are we seeing another significant shift in cyber norms and rules of engagement?

Cyber Attacks & Physical Infrastructure: Examples

APRIL 26, 2020 6:28 PM 1

Israel Thwarts Major Coordinated Cyber-Attack on Its Water Infrastructure Command and Control Systems

by Benjamin Kerstein

Shamoon virus returns in Saudi computer attacks after four-year hiatus

By Jim Finkle, Tom Finn and Jeremy Wagstaff

December 1, 2016 3:42 PM EST · Updated 8 years ago

- Saudi Aramco 2012: Partially wiped or destroyed 35,000 computers
- 2013 Bowman Dam
- Colonial Pipeline 2021 ransomware attack
- 2021 Florida Water treatment
- 2022 Viasat attack
- Salt Typhoon and telecoms
- Ransomware targeting healthcare institutions

Opening Pandora's Box?

“This is the most extensive, publicly-known physical supply chain attack we’ve ever seen, may even see for a while,” said Dmitri Alperovitch, chair of Washington-based geopolitics think tank Silverado Policy Accelerator and co-founder of cybersecurity firm CrowdStrike.
https://www.politico.com/news/2024/09/19/pager-attacks-supply-chain-warfare-00180136

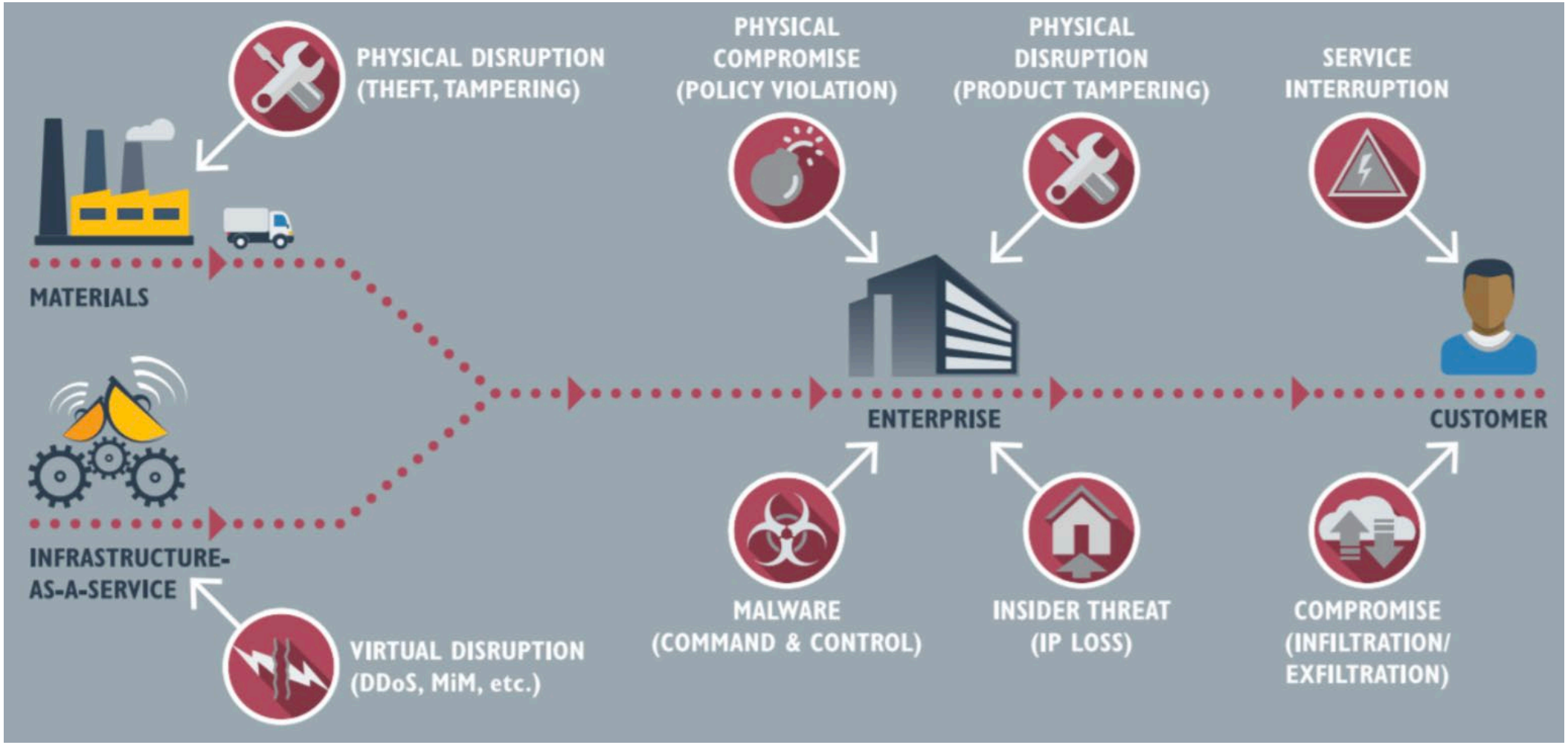
RSAC 2025 Conference

Technical Supply Chain Infiltration

Brief Overview

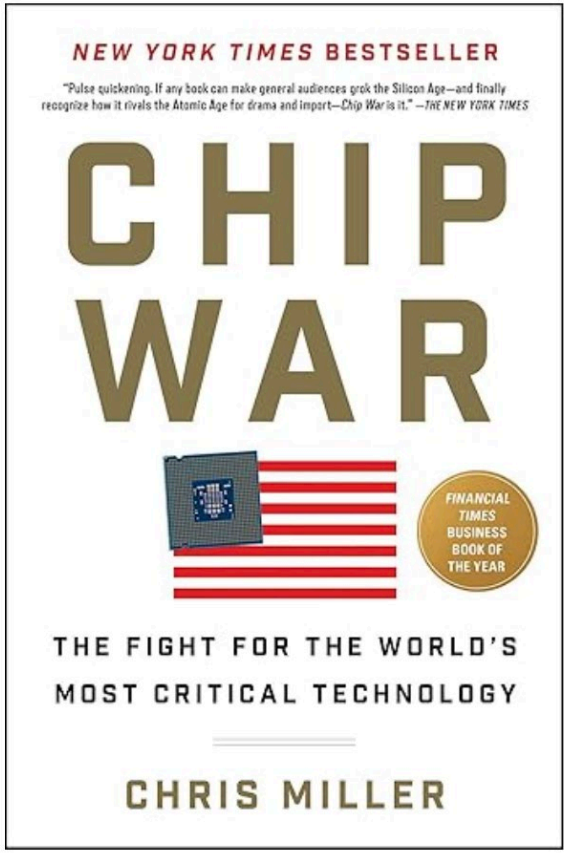
Many Voices.
One Community.

Physical versus Virtual Infiltration



https://d3.harvard.edu/platform-rctom/submission/target-under-attack/

The Risk of Hardware Tampering


NEW YORK TIMES BESTSELLER
"Pulse quickening. If any book can make general audiences grok the Silicon Age—and finally recognize how it rivals the Atomic Age for drama and import—Chip War is it." —THE NEW YORK TIMES
CHIP WAR
FINANCIAL TIMES BUSINESS BOOK OF THE YEAR
THE FIGHT FOR THE WORLD'S MOST CRITICAL TECHNOLOGY
CHRIS MILLER

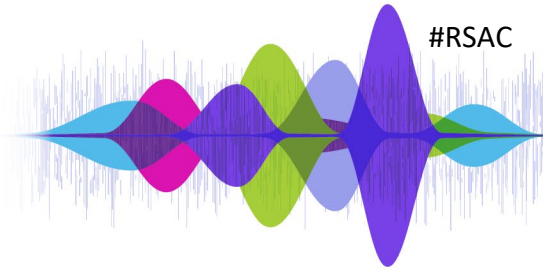
"Companies have spent the past two decades building defences against cyber attacks, spending billions in the process.

Yet even the most sophisticated of them devote few resources to verifying the chips or inspecting the circuit boards inside their systems.

Some manufacturers still fail to monitor the origin of components deep in their supply chains, despite the creation of powerful software to facilitate this."

https://www.ft.com/content/5c8f5c51-e205-4213-a85a-e6c52963c72c

Supply Chain Compromise: Compromise Hardware Supply Chain



"Adversaries may manipulate hardware components in products prior to receipt by a final consumer for the purpose of data or system compromise. By modifying hardware or firmware in the supply chain, adversaries can insert a backdoor into consumer networks that may be difficult to detect and give the adversary a high degree of control over the system."

ATT&CK®

Supply Chain Compromise: Compromise Hardware Supply Chain

Supply Chain Sub-Threat Vectors

Counterfeit Components

Counterfeit components are more susceptible to cyber-attack and are more likely to break because of their poor quality. Compromised counterfeit components could enable a malicious actor to impact the confidentiality, integrity, or availability of data that travels through the devices and to move laterally to other more sensitive parts of the network.

Inherited Components

Inherited components may come from extended supply chains consisting of third-party suppliers, vendors, and service providers. Supply chains may be compromised via attacks on suppliers, including suppliers of suppliers, who may have weaker security controls and audits on their development, production, or delivery channels. Flaws or malware inserted early in the development phases are more difficult to detect and could lead to the developer marking the component as legitimate through digital signatures or other approvals. These vulnerabilities could then later be exploited by malicious actors.

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

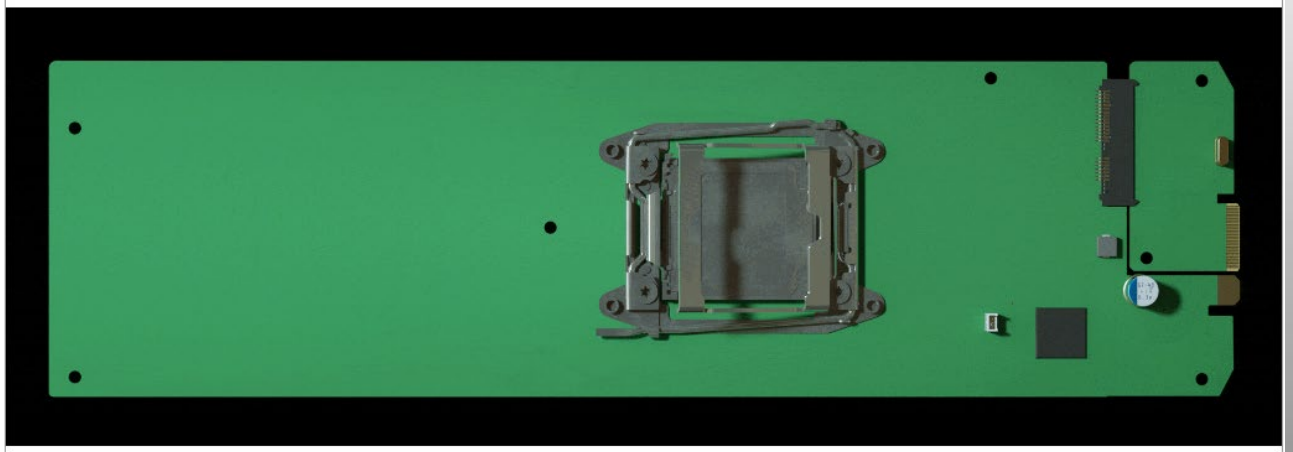
https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%2520%25281%2529.pdf

Spy Chip-Gate?

Businessweek | Feature

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.



Illustrator: Scott Gelber for Bloomberg Businessweek

By Jordan Robertson and Michael Riley
October 4, 2018 at 5:00 AM EDT

Save Translate

This article is part of the **October 8, 2018 issue** of Businessweek.

The Long Hack: How China Exploited a U.S. Tech Supplier

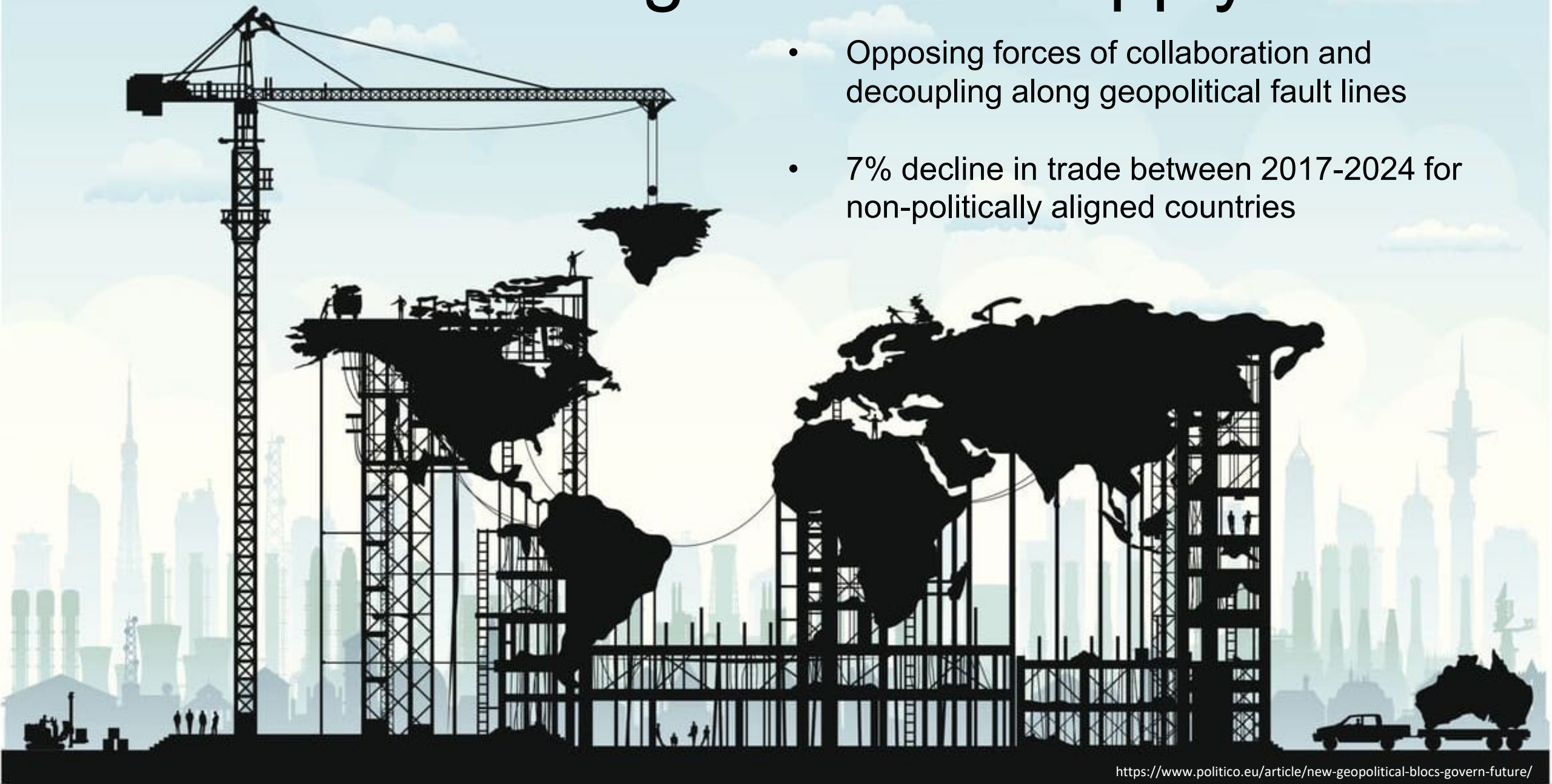
For years, U.S. investigators found tampering in products made by Super Micro Computer Inc. The company says it

RSAC 2025 Conference

Untrustworthy Networks: Global Tech Bifurcation & Supply Chain Risks

Reglobalized Supply Chains:

- Opposing forces of collaboration and decoupling along geopolitical fault lines
- 7% decline in trade between 2017-2024 for non-politically aligned countries



https://www.politico.eu/article/new-geopolitical-blocs-govern-future/

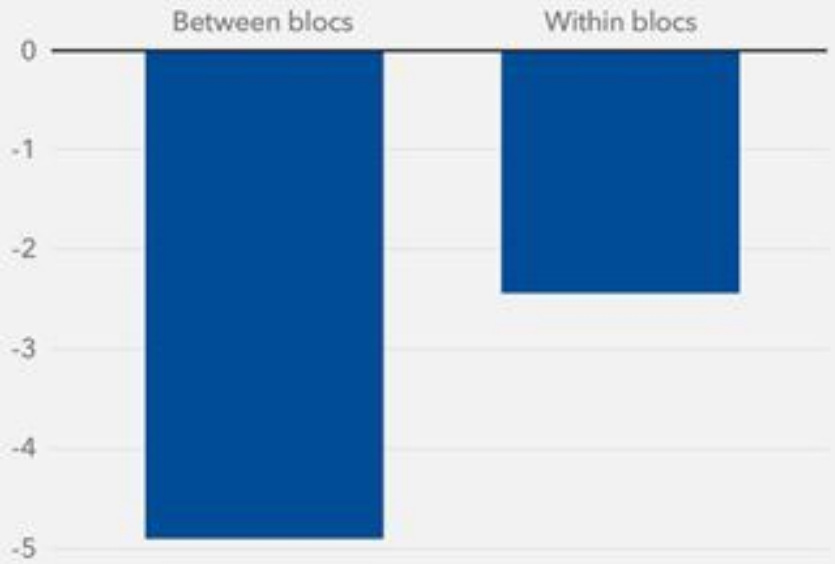
Geopolitical Fault Lines

EMERGING FAULT LINES

GEOPOLITICAL CONSIDERATIONS ARE ALREADY AFFECTING TRADE FLOWS

CHANGE IN TRADE GROWTH POST WAR

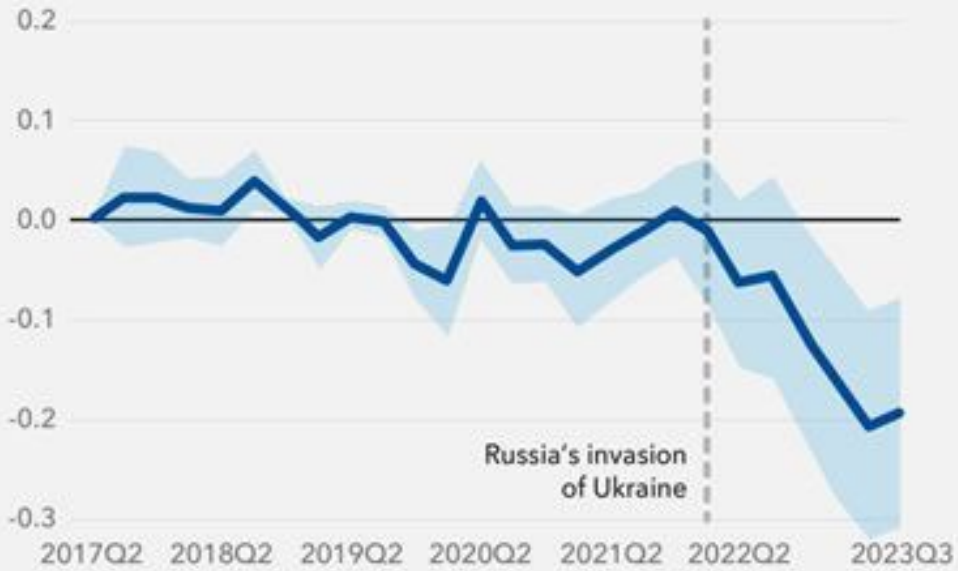
(PERCENTAGE POINTS)



Source: Gopinath et al. (2024), Trade Data Monitor and IMF staff calculations
Note: The chart shows the weighted quarterly trade growth averaged over quarters during 2022Q2 - 2023Q3 minus the equivalent for the period 2017Q1 - 2022Q1 within blocs, and between blocs.

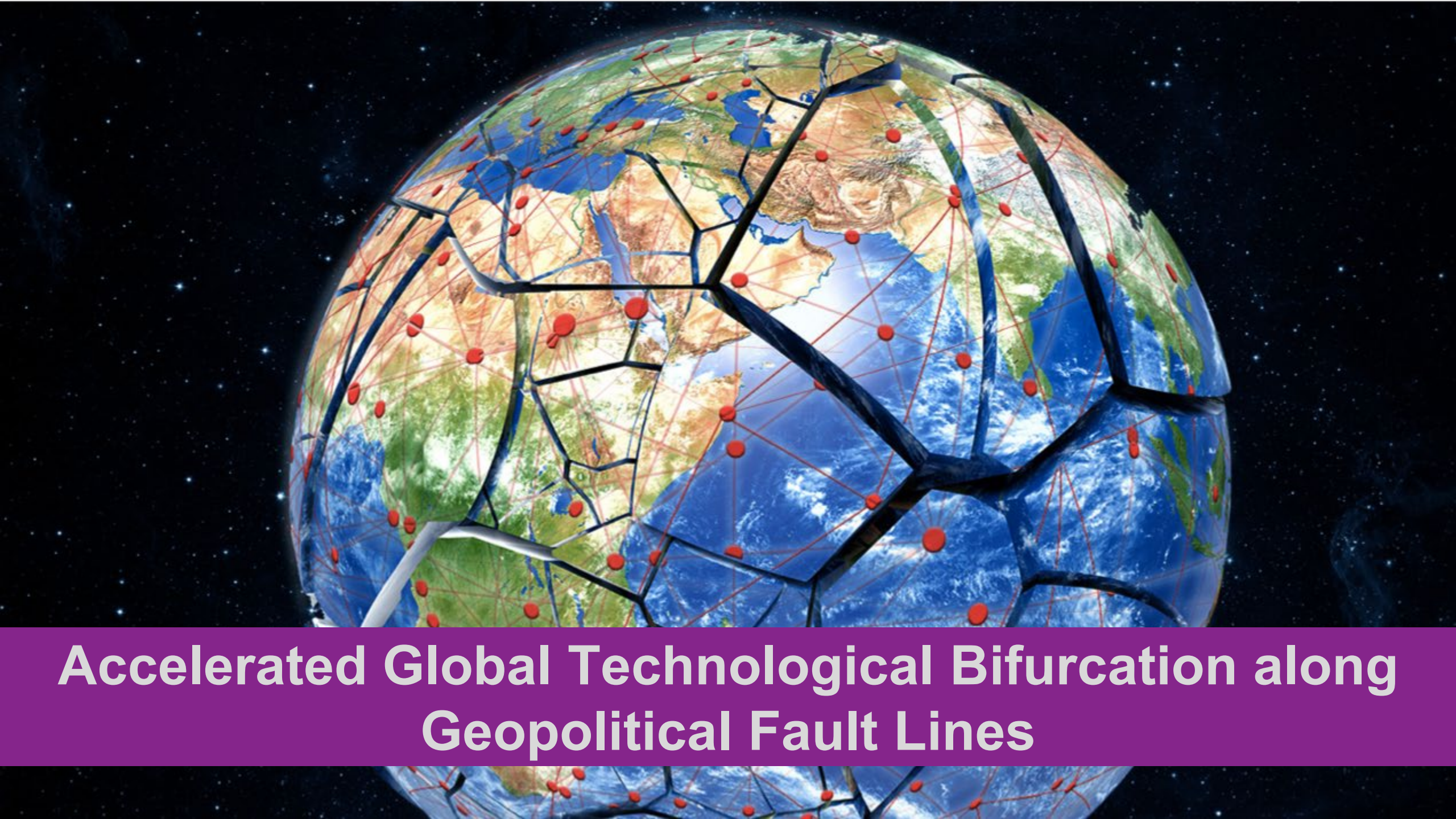
TIMING OF TRADE FRAGMENTATION, BETWEEN BLOCS

(SEMI-ELASTICITY)



Source: Gopinath et al. (2024), Trade Data Monitor and IMF staff calculations.
Note: Plots the semi-elasticity of trade for flows between blocs, and associated 90 percent confidence bands, estimated with PPML and a fully saturated gravity model. Bloc definition based on Ideal Point Distance (a measure based on voting pattern in the United Nation General Assembly computed by Bailey et al. (2017)).

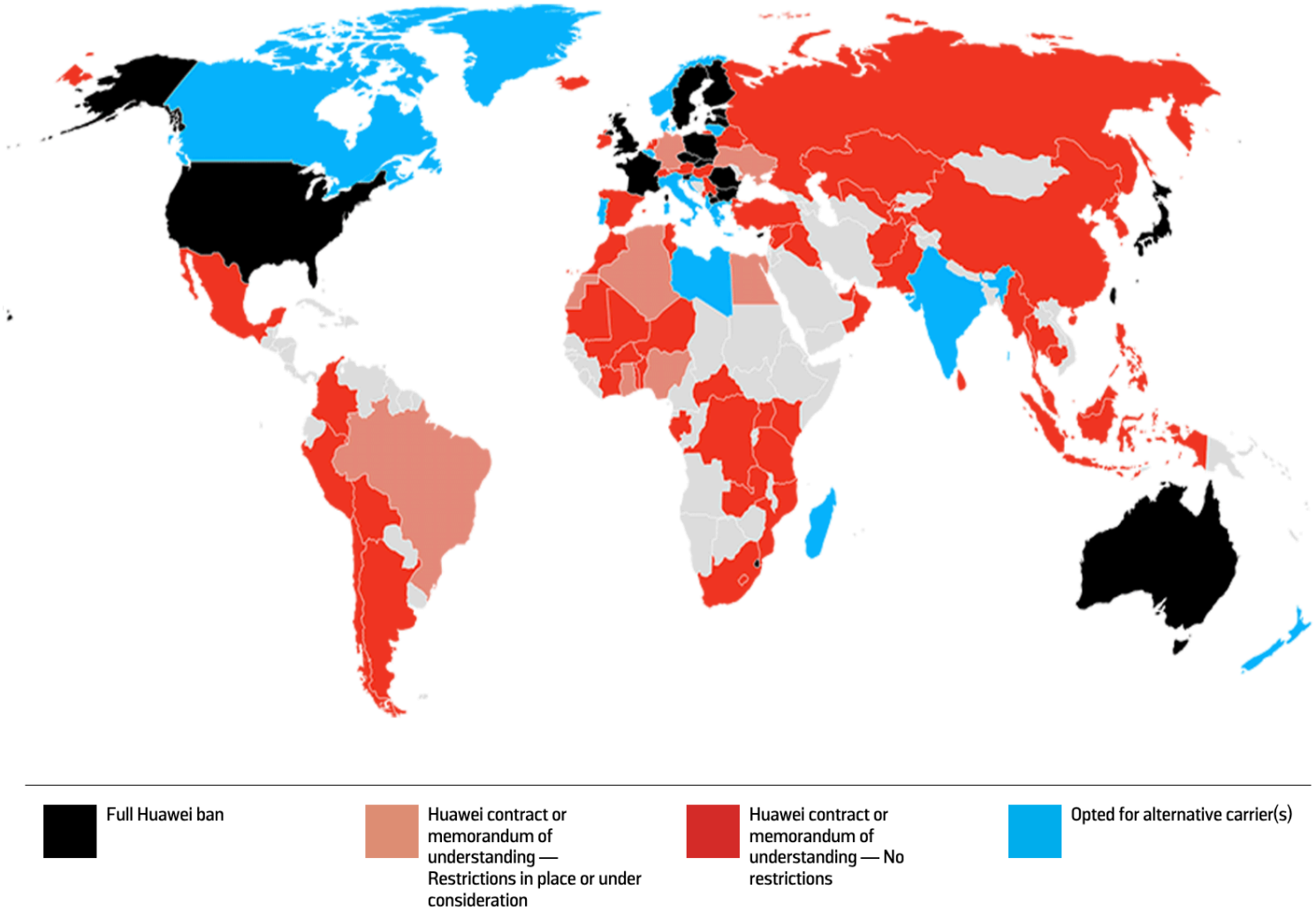
https://www.ft.com/content/5b50af30-ff54-47bf-a2f9-c8f118361fcd



Accelerated Global Technological Bifurcation along Geopolitical Fault Lines

Bifurcation of Technologies: 5G

Despite being pushed out of key EU markets in 2020, Huawei maintains a strong global presence across Asia, Africa, and Latin America


Full Huawei ban
Huawei contract or memorandum of understanding — Restrictions in place or under consideration
Huawei contract or memorandum of understanding — No restrictions
Opted for alternative carrier(s)

https://foreignpolicy.com/2020/01/22/5g-cellular-huawei-china-networks-technology-infrastructure-power-map/

Bifurcation of Technologies: Drones

GEORGIA TO BAN CHINESE DRONES IN MAJOR SECURITY PUSH

Haye Kesteloo / February 17, 2025 /
China, Data Security, Department Of Defense, Department Of Transportation, Georgia, New Jersey, Russia, Walmart, White House /
1 Comment

DJI drones escape US ban for now, but clouds continue to loom for 2025

News By Alex Blake published December 19, 2024

To ban or not to ban

When you purchase through links on our site, we may earn an affiliate commission. Here's how it works.

- China controls ~80% of the drone market
- Tit-for-tat export controls between China and the US

Decision on Taking Countermeasures Against U.S. Military Companies and Senior Executives

Updated: DECEMBER 05, 2024 19:45

(Issued on December 5, 2024 as Decree of the Ministry of Foreign Affairs ofthe People's Republic of China No. 14, effective as of December 5, 2024)

Recently, the United States announced another arms sale to China's Taiwan region. This seriously violates the one-China principle and the three China-U.S. Joint Communiqués, interferes in China's internal affairs, and undermines China's sovereignty and territorial integrity. Pursuant to Articles 3, 4, 5, 6, 9 and 15 of the Law of the People's Republic of China on Countering Foreign Sanctions, China hereby decides to take countermeasures against the following U.S. military companies and senior executives:

For the 13 companies listed in the attached List of Targets of Countermeasures, i.e., Teledyne Brown Engineering, Inc., BRINC Drones, Inc., Rapid Flight LLC, Red Six Solutions, Shield AI, Inc., SYNEXXUS, Inc., Firestorm Labs, Inc., Kratos Unmanned Aerial Systems, Inc., HavocAI, Neros Technologies, Cyberlux Corporation, Domo Tactical Communications, and Group W:

Their movable and immovable properties, and other kinds of assets within China shall be frozen.

Bifurcation of Technologies: AI

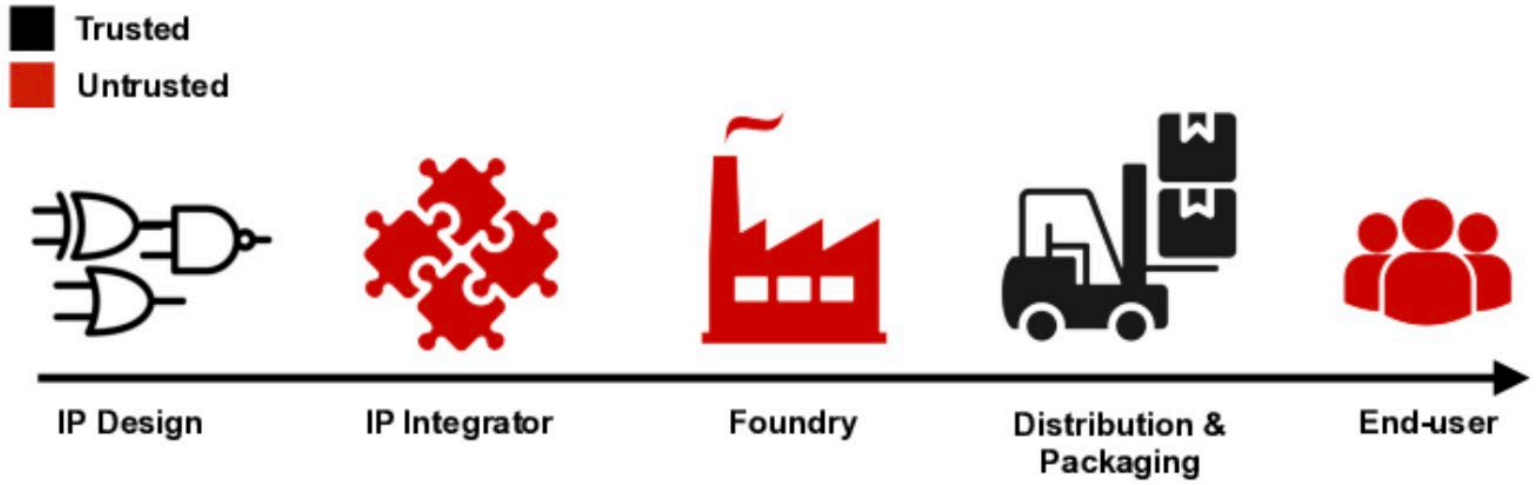
- The DeepSeek Disruption:
  - Most downloaded app in history, followed by various limitations, bans, or investigations in South Korea, Taiwan, US, Italy, Australia, Belgium, Ireland, and France
- OpenAI restricting API traffic from countries where the services are not supported

Singapore Scheme May Have Funneled Nvidia Chips to DeepSeek

Three people, including one Chinese national, were charged with conspiracy to commit fraud.

Bifurcation of Technologies: Semiconductor Supply Chains

- Complex and hyperspecialized and concentrated supply chain
- Growing illegal market of chips flowing into China to circumvent export controls introduces heightened risks of counterfeit and tampering
- Tit-for-Tat export controls on companies, critical minerals



Horizontal model of supply chain for the semiconductor industry.

Other Modes of Tech Infiltration

WAR ON THE ROCKS — National security. For insiders. By insiders.

RUSSO-UKRAINIAN WAR ABOUT SIGN IN

THE RISE OF THE FAKE TECH WORKFORCE: STATE-SPONSORED INFILTRATION OF U.S. TECHNICAL SUPPLY CHAINS

NATHANIEL DAVIS AND NINA KOLLARS

FEBRUARY 27, 2025

COMMENTARY

- "On Dec. 12, 2024, the Department of Justice released an indictment against 14 North Korean nationals for involvement in a fake IT worker scheme impacting hundreds of U.S. firms and funneling millions of dollars to the ballistic missile program in the Democratic People's Republic of Korea."

“The scientific and technological revolution and the great power game are intertwined.”
Chinese President Xi Jinping at the National Science and Technology Awards Conference 2024

RSAC 2025 Conference

Looking Ahead

Derisking supply chains during geopolitical uncertainty & evolving cyber norms

Many Voices.
One Community.

A New Era of Cyber Norms?

- After six months, there has not yet been similar supply chain tampering based on physical destruction and lethality
- Potentially similar cases in Russia
  - JAN-FEB 25: Reported by State Media, Russian soldiers received drone headsets that exploded when turned on
  - Delivered as humanitarian aid

In Mossad Pager-Style Operation, Russian Drone-Control Goggles Explode, Blinding Soldiers

The booby trapped goggles were delivered as "free aid" to the Russian army by suspected Ukrainian intelligence operatives.

Defensemirror.com bureau 11:12 AM, February 19, 2025 2036

Russian FPV pilot @via open sources

https://www.defensemirror.com/news/38880/In_Mossad_Pager_Style_Operation__Russian_Drone_Control_Goggles_Explode__Blinding_Soldiers

A New Era of Cyber Norms?

- Uncertainty persists, inserting geopolitical considerations into board rooms and supply chain risk management

The New York Times

GUEST ESSAY

Israel's Pager Attacks Have Changed the World

Sept. 22, 2024

Mohammad Zaatari/Associated Press

Share full article 272

By Bruce Schneier

Mr. Schneier is a security technologist and a lecturer at the Harvard Kennedy School.

Key Considerations

- Economic, financial, and supply chain fragmentation introduce new risks as well as shifts in efficiency, costs, and volatility
- Norms are reshaping supply chain risks, including tampering, counterfeits, and other manipulation
- The pace of technological innovation is advancing rapidly, introducing both opportunities and risks
- Identify any geographic and product dependencies within your supply chain
- Review identity validation and hiring processes
- Building trusted networks during shifting cyber norms and tampering

Steps on Derisking Your Supply Chain

- Next week you should:
  - Integrate a geopolitical lens when approaching tech strategies and competition and opportunities and risks associated with it
- In the first three months following this presentation you should:
  - Identify any geographic or product dependencies with specific concentration risks, especially in areas of growing political risk
  - Assess supplier vetting and identity validation processes, as well as hiring
  - Integrate supply chain tampering and manipulation risks into cross-department conversations
  - Monitor cyber escalation in your networks but also globally for shifting cyber behavior
- Within six months you should:
  - Have a diversification and resilience strategy based on trusted networks, including identified geographic dependencies or at-risk products
  - Collaborate across departments for common understanding and approach to supplier validation
  - Anticipate uncertainty as the new norm

RSAC™ 2025 Conference

Many Voices.
One Community.